Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Bridging the gap between Red-alert virus situation and quality file-signature release

Recently, antivirus vendors have come under increasing criticism about the time they take to react to a red-alert virus situation1. Virus' have become more sophisticated and spread more rapidly than ever before. Correspondingly, antivirus vendors are required to reduce the time taken to respond to new viruses. They also need to continue to provide quality support. Thus, balancing the need for a quicker solution with the market requirement for quality solutions and support. This has highlighted the need for both a parad...

Copyright SANS Institute
Author Retains Full Rights

AD

Bridging the gap between Red-alert virus situation and quality file-signature release

Ken Millard
4th November 2002

Abstract

Recently, antivirus vendors have come under increasing criticism about the time they take to react to a red-alert virus situation[1]. Virus' have become more sophisticated and spread more rapidly than ever before. Correspondingly, antivirus vendors are required to reduce the time taken to respond to new viruses. They also need to continue to provide quality support. Thus, balancing the need for a quicker solution with the market requirement for quality solutions and support. This has highlighted the need for both a paradigm shift in malware protection and investment in new technology to implement this shift.

It is no longer sufficient to only have the mechanism to provide worldwide automatic downloads of product updates to meet head-on any virus threat. The antivirus vendors must also produce these updates in a timely, quality controlled manner. This paper will look at the reasons behind this change, how it came about and how technologically the protection needs can be addressed. It will also briefly look at the possible economical advantages of adopting such technology.

History of antivirus updates

Firstly, it needs to be understood that antivirus vendors must write a new signature for each new virus[2]. Before 1995 most viruses spread via floppies and network servers. During this period, the effective spread rate are best epitomised by FORM. This virus took 6 years to become the most prevalent virus of its time. Faced with this kind of threat, the need for antivirus product updates, i.e. new signatures, was more than adequately met with a combination of floppies and snail-mail. These floppies were distributed on a quarterly basis. However, if you were willing to invest more, or were simply more paranoid, these could be delivered on a monthly basis[3]. For example, every week thousands and thousands of floppies were distributed by the likes of S&S Software (a.k.a. Dr Solomon's Software) to satisfy this need. The products themselves had some automatic update facilities but they often required a degree of manual intervention. Subsequent years saw a phenomenal growth in the number of macro viruses. Many virus writers decided to follow the example of the Concept[4] virus, created in August 1995. During the same period E-mail started to become

[1] Peter Tippet
[2] Schneier
[3] Tranton
[4] Concept Virus

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

the means of choice for the distribution of both normal and infected attachments. The subsequent exponential growth in the use of the same E-mail added further to the impact and indeed distribution of said viruses. Overall, the quickening of virus distribution necessitated that antivirus vendors automate their updating mechanisms. Like viruses, the obvious choice for a distribution mechanism was the Internet. Antivirus vendors invested in placing the required technology inside both their products and in backbone technology to provide antivirus solution updates on a weekly cycle.

Rapid infections

However, the rapidity of virus distribution continued unabated, culminating in viruses such as W97M_MELISSA.A[5] / VBS_LOVELETTER[6] / CODERED[7]. By combining social engineering and automatic distribution (and other technologies) these viruses have continued to increase the infection rate. They have reached an infection rate of over a quarter of a million PCs in nine hours[8], see Figure 1.

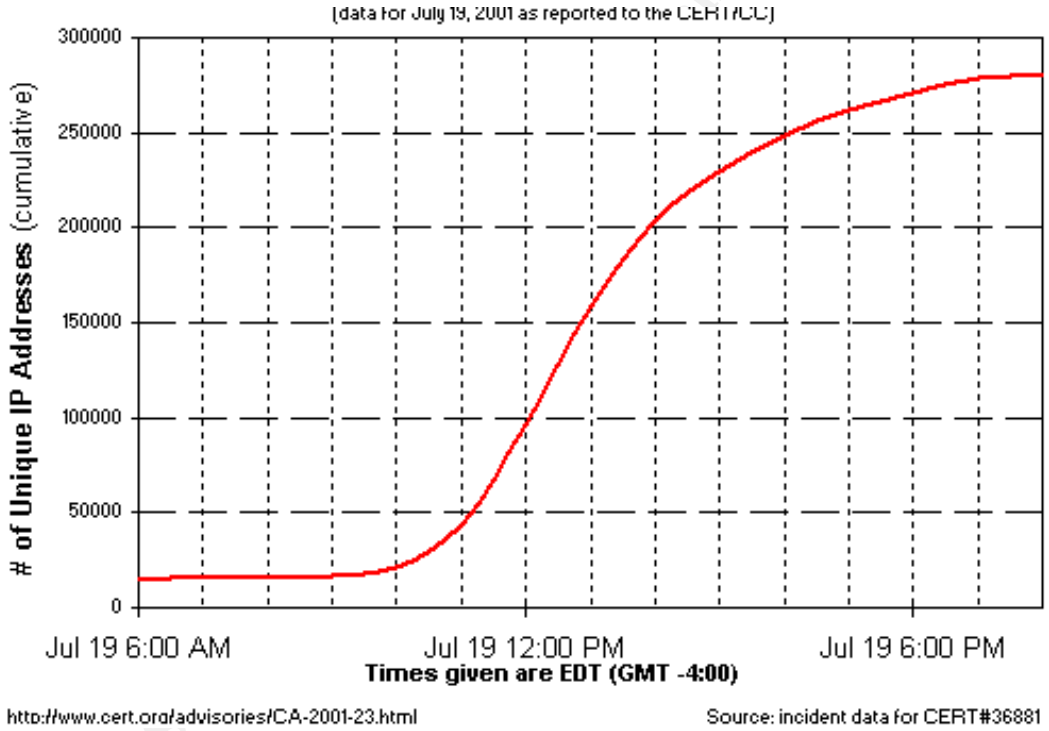

Figure 1: Graph of the infection rate of Codered in July 2001

Clearly, weekly updates do not work in these kinds of situations.

"Original AV scanners had six-month, quarterly and then monthly updates of

[5] W97M_MELISSA
[6] VBS_LOVELETTER
[7] CODERED.A
[8] CERT/CC

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

signatures. This simply isn't enough. The lifecycle of an attack capitalising on known vulnerabilities continues to accelerate, so customers need automated updates on a daily or even an hourly basis. This can only be accomplished through the latest automated tools that detect and fix system vulnerabilities before malicious attackers can exploit them."[9]

Antivirus vendors have had to produce product updates in a very short space of time. Also these updates must be of a sufficient quality so as not to introduce more problems than the original virus.

Antivirus vendor reaction

Antivirus vendors organised themselves to react to these new alerts. To help organise their response according to threat they specified criteria for types of alert and subsequent reactions. For example, Trend Micro Inc. defined red-alert as reports of infection from three countries and yellow alert as two such reports. Trend created a Rapid Response Team as advocated by Roger A. Grimes[10] to react to these classified threats. The original job of this worldwide team was to co-ordinate the effort of providing the solution. In parallel they communicated with the media and customers/channel the details of the threat and its solution. Combining the threat and the solution is of prime importance in this period otherwise the hype and scare mongering will know no limits. Additionally, the lack of solution makes the virus warning seem like a virus hoax. This in turn does little to garner respect for the antivirus vendors who might start to be accused of crying wolf.

This response task was, in itself, daunting enough. Viruses do not respect the concepts of day and night and often these teams have to work through the night to be ready for a virus that would "hit" the next morning. In addition to this, they have to react, not only to the original version of the virus, but also to the 10s of bandwagon variants that appear soon after. For example, some of the KLEZ variants have become more "important" than the original[11]. In the case of the LOVELETTER virus, 7 updates were required in the subsequent 24-hour period to counter the rapidity of the bandwagon jumping! This number of updates in such a short space of time places immense stresses on an already complicated process. Combining the creation of a complicated solution with a too strict a time constraint could lead to quality difficulties.

[9] Armstrong, Amer Deeba Section
[10] Roger A. Grimes, Page 436
[11] Virus Bulletin

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Quality

A few antivirus vendors have already implemented quality procedures[12] into their solution providing process. Their first aim was to meet the requirements of customers for quality support. Secondly, these processes also help to avoid the antivirus solution causing problems with false-positives and false-negatives. In a nutshell, they were trying to avoid the virus problem becoming an antivirus problem.

As a fundamental part of any antivirus package, additions of new virus signature(s) need to be tested. This testing must encompass a whole raft of platforms and multiple application situations to limit as much as possible the negative impact of a badly written virus signature. This implies that the gap between the time a virus goes into red[5]- or, indeed, yellow-alert mode and the time a fully checked pattern file, that properly identifies this virus/malware, makes it to general distribution will be unlikely to reduce significantly.

Antivirus costs

The main factor that is driving this effort is the cost involved in antivirus operations. Figure 2 shows the relative costs are heavily imbalanced towards the assessment and clean-up phases of the operation.

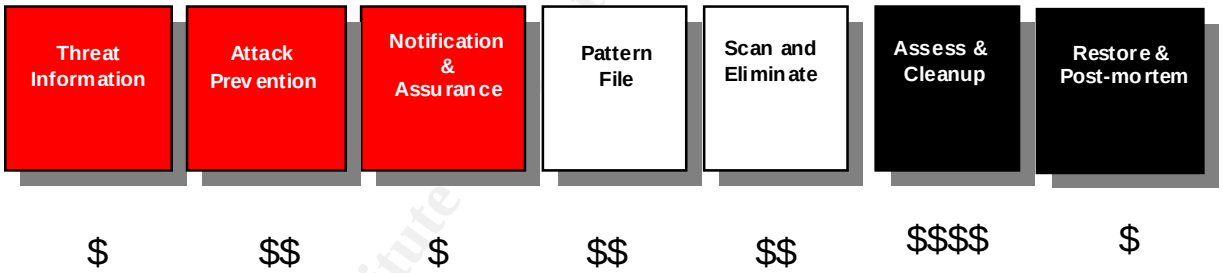

Figure 2: Relative costs of a virus infection

We can see that, when trying to reduce these costs, prevention is obviously better than cure. In fact, Computer Economics estimated in 2001 that 80% of outbreak costs are related to cleaning[13]. Thus, a combined need for an improved time to solution with keeping the costs of an outbreak to a minimum has created a growing demand for solutions such as Trend Micro's Enterprise Protection Solution.

[12] **ISO 9002 Certification**

[13] Computer Economics, 2001

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Improved time to solution

To address this and to improve the time to solution Trend Micro Inc. has added new technology into its automated download systems and, equally importantly, into the products themselves. This technology adds the ability to react, albeit temporarily, to a red or yellow-alert situation. The configuration changes required to react can be produced without compromising the quality control standards. At the same time it provides for a more secure solution for their time-pressed customers.

Update security

To improve the security within a solution of this kind must guard against the following risks

1) the download of a falsified OPP by the central manager
2) the acceptance of a falsified OPP by the various antivirus/content checking solutions

The risks here are:

1) the data integrity has been compromised by hijacking the communication process between server and client
2) the client is talking with a server that is not the correct server
3) the information about the configuration of the antivirus/content checking software can be intercepted during transmission

For example, Trend's Control Manager product offers 6 combinations of different encryption and key exchange mechanisms for OPP transmission within an organisation. The choice of encryption and identification method will depend on the risk and threat associated with sending these configuration vectors over the necessary lines of communication between the central product and each of the peripheral AV/Content Filtering solutions. In the case of Control Manager the options are:

1) No SSL encryption
2) 40-bit SSL encryption
3) 128-bit SSL encryption
4) One-way end-to-end authentication with no SSL encryption
5) One-way end-to-end authentication with 40-bit SSL encryption
6) One-way end-to-end authentication with 128-bit SSL encryption

When the server is installed a public and private key pair are created. The public key is passed to the antivirus/content checking solution during registration of the product. This public key is used to authenticate the server.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

New approach

Due to the previously discussed paradigm shift in virus distribution mechanisms, antivirus companies must find a solution that matches, if not betters this. The automatic update process implemented throughout the Trend Micro product range for a number of years is now no longer enough. We must be aware that any new automated solution needs both product modifications and back-room technology to achieve a workable solution. Trend Micro has already implemented the back-room technology as part of its Enterprise Protection Strategy[14]. Various products need to be capable of implementing the preventative measures that have been prescribed to limit the impact of the new virus! The following table (Figure 3) demonstrates the kind of actions the various product families need to be capable of performing to implement the preventative or shielding measures contained in the OPP[4].

Product Family	Port blocking	Attachment blocking	Content checks	File system protection	Real-time scan activation	URL/WEB server blocking	Share Blocking
Client	✓	×	×	✓	✓	×	✓
Server	✓	×	×	✓	✓	×	✓
GroupWare	×	✓	✓	×	✓	×	×
Gateway	✓	✓	✓	×	✓	✓	×

Figure 3: Available protection mechanisms

Please note that the product family refers to the type of antivirus product and not to the type of platform. Thus, a server product could, and should, be installed on the same hardware as the groupware product.

Some of these new features add a degree of firewall protection to a computer but their intention is not to replace any existing firewall measures but simply to add to the antivirus protection.

Virus' activity vs. virus activity

To be able to identify and act upon virus' activity as opposed to virus activity offers significant benefits in reducing the spread and impact of a virus. If a virus has already penetrated the boundary protection mechanisms its activity must be controlled until the proper antidote is ready and implemented. For example, if a certain active virus sets up a process on a certain port that floods the network with SYN/ACK attacks then the antivirus can, when instructed to do so by the OPP, block that port and prevent the virus from continuing with its DoS efforts.

[14] **Enterprise Protection Strategy**, **Trend Micro INC, 2002**

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Solution complexity

Specifying these types of rules for the various product groups is a much simpler process and does not need the technical product know-how that modifications to most virus patterns require. Most virus patterns are written in complex machine-code type languages that require in-depth proprietary knowledge to write/modify. Hence the need for rigorous quality controls. On the other hand, the OPP does just what its name implies; it tries to prevent the outbreak from spreading any more than it already had done when the OPP was downloaded. Due to its nature, a red-alert team only has a limited crisis time available. They can focus on gaining a more complete understanding of the virus the first time and getting the prevention policy in place. This does not remove the equally urgent need for the team to provide a "traditional" file pattern to detect and remove the malware.

Security product

Good security covers prevention, detection and reaction[15]. Looking at this type of solution in these terms we find that:

1) the prevention of viruses from entering the company is improved, as is the spread of a virus that has already penetrated the outer defences.
2) early detection of viruses is improved due to reducing the initial reliance on a complex file pattern signature that needs more time to produce in a quality manner.
3) notification of both virus' activity and virus activity are fundamental parts of this solution. The ability to pinpoint the entry-point and distribution paths of a virus and work directly on these even remotely is of course essential[16].

[15] Secrets and Lies, Page 8
[16] Mobile Malicious Code, Page 453

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Example OPP

The WORM_bug_bear.a[17] virus combined a variety of malware attacks and software loopholes to become the most infectious and damaging malware in 2002. A simplified Outbreak Prevention mechanism for this malware can do all of the following:

For clients and network servers:	Blocking port 36794 Set network shares to read only Block the creation of ~PHGGUM.TMP and ~EAYLNLF.TMP
For IIS web servers:	Closing down port 36794
For E-mail servers:	Attachment setup.exe; sender boxhill@teach.com
For Content Management servers:	Subject: Just a reminder
For Web gateways:	Blocking access to any port 36794

The administrator can opt to implement or not these various options.

Potential savings

(For the sake of simplicity I am assuming that the infection rate is linear.)

Worldwide costs of virus infections are estimated at $10.7B, Jan-August 2002[18]. Clean-up costs are said to be 80% of this total, i.e. $8.6B. If we were, very conservatively, able to decrease the time of implementing preventative measures by 50% and these, in turn were capable of reducing the spread and impact of an infection by 50%, then this would represent a saving, for this period, of $2.2B!

Looking at a specific example, NIMDA costs are estimated at $530M[19]. Clean-up costs would be $424M. Applying our improvement measure to this we would in this case have saved $112M for one red-alert outbreak.

The Computer Security Institute 2002 survey found that the average annual cost for virus infections in a company was $283,000[20]. Applying the saving calculation above, each company would thus expect extra savings of $57,000 per year.

[17] Worm_bug_bear.a
[18] Computer Economics
[19] Taming Nimda
[20] Computer Security Institute

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Conclusion

In the current rapidly moving environment, anything, which reduces the time between virus outbreak and solution implementation, is a welcome addition to any antivirus administrators armoury. The introduction of capabilities to limit already spreading viruses will help further reduce the costs involved in a virus outbreak. Such restrictions can isolate an infected PC/server from the rest of the network and, in doing so, limit any further spread of the infection until such time as the proper automatic process included in the resident antivirus product can neutralise it. The effect of properly implementing such a policy will be to significantly reduce both the effect that a virus outbreak has on an organisation and the costs involved in repairing the subsequent damage.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

List of references

1. Tippet, Peter. "The Great AV Myth". Information Security, September 2001: 36.
2. Schneier, Bruce. Secrets and Lies - Digital Security in Networked World, Wiley Computer Publishing, 2000. 154.
3. Tranton, Shawn (Ed.), "Virus News", SSS, June 1997, URL: http://www.vibert.ca/vn97006.pdf
4. Trend Micro, "Concept", Trend Micro Virus Encyclopaedia, Sept 1998, URL: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WM_CONCEPT
5. Trend Micro, "W97M_Melissa", Trend Micro Virus Encyclopaedia, Aug 1999, URL:http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=W97M_MELISSA
6. Trend Micro, "VBS_Loveletter", Trend Micro Virus Encyclopaedia, May 2000, URL:http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=VBS_LOVELETTER
7. Trend Micro. "CodeRed.A". Trend Micro Virus Encyclopaedia, July 2001, URL: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=CODERED.A.
8. CERT/CC, 'CERT® Advisory CA-2001-23 Continued Threat of the "Code Red" Worm', January 17, 2002, URL: http://www.cert.org/advisories/CA-2001-23.html.
9. Armstrong, Illena. "Automating Security: Removing the Human Factor". SC Magazine, 2002, June: Special Feature, Section by Amer Deeba – Automating the Pillars of Security.
10. Grimes, Roger, A. Malicious Mobile Code – Virus Protection for Windows. O'Reilly, August 2001: 436
11. Virus Bulletin, "W32/Klez", Virus Bulletin Virus Resources, 2002, URL: http://www.virusbtn.com/resources/viruses/indepth/klez.xml, 23/11/2002
12. Trend Micro, "ISO 9002 Certification", Trend Micro Earns ISO 9002 Certification for Antivirus Research and Support Operations, Jan 31 2001, URL: http://www.trendmicro.com/en/about/news/pr/archive/2001/pr013101.htm
13. Computer Economics, Achieving a Positive ROI on IT Security 2001, URL: http://www.computereconomics.com/article.cfm?id=668. Paper only available on subscription.
14. Trend Micro, Enterprise Protection Strategy, September 2002. URL: http://www.trendmicro.com/en/products/eps/features.htm
15. Schneier, Bruce. Secrets and Lies - Digital Security in Networked World, Wiley Computer Publishing, 2000. 8.
16. Grimes, Roger, A. Malicious Mobile Code – Virus Protection for Windows.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

O'Reilly, August 2001: 453
17. Trend Micro. "CodeRed.A". Trend Micro Virus Encyclopaedia, Sept 2002. URL: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_BUGBEAR.A&VSect=T
18. Trusecure, Taming Nimda, August 2002, URL: http://www.trusecure.com/download/dispatch/taming-nimda.pdf?ECDE=W0072&CMP
19. Computer Economics, 2002, URL: http://www.computereconomics.com. Paper only available on subscription.
20. Computer Economics, 2002. The Computer Economics Security Review 2002 (April 2002). URL: http://www.computereconomics.com/article.cfm?id=356. Paper only available on subscription.
21. Computer Security Institute, 2002 CSI/FBI Computer Crime and Security Survey, Computer Security Issues and Trends, Volume VIII. No.1, Spring 2002, URL: http://www.gocsi.com/pdfs/fbi/FBI2002.pdf

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**